

In the POTS environment, where all of the communications associated with a particular telephone number ordinarily could be detected over the subscriber's local loop, there was no reason for purposes of Title III interception orders (or judicial opinions analyzing such orders) to distinguish the telephone number from the physical equipment connecting the subscriber to the carrier. See Government June Comments at 28-29. In digital networks, by contrast, a subscriber's features and services may result in communications that have no detectable effect upon the subscriber's terminal equipment because the features and services are activated and implemented at the switch. Interception orders for switch-based electronic surveillance therefore may define the "facility" under surveillance functionally, by reference to the services associated with a particular telephone number or account. For example, a subscriber who invokes call forwarding will not receive calls at the terminal associated with his telephone number, but an interception order directed at the subscriber's "facilities," defined by reference to his phone number or any other description that satisfies the particularity requirement of the Fourth Amendment (as articulated in Title III by the phrase, "nature and location"), would authorize law enforcement to intercept the forwarded call at the switch. And it is equally clear that Section 103(a)(1) of CALEA requires carriers to have the capability to provide law enforcement with the content of such forwarded calls. See House Report at 9, reprinted in 1994 USCCAN at 3489; see also J-STD-025, § 5.4.7 (Redirection message); *id.* Annex D, § D.11. The commenters' insistence that Title III "facilities" are restricted to a particular subscriber's terminal equipment is therefore incorrect.¹²

¹² However, we are not suggesting (as some commenters claim) that a Title III "facility" could encompass "the entire network to which [a] telephone is attached." PCIA Comments at 24. A Title III facility is confined to the network elements that support and are identifiable with the services (continued...)

B. Party Join/Hold/Drop Information

The J-Standard does not require carriers to notify law enforcement when parties join a multi-party call, drop from the call, or are placed on hold. The Commission has tentatively concluded that the J-Standard is deficient in this regard and must be modified to ensure that carriers provide law enforcement with reasonably available party join, party hold, and party drop information. Notice ¶¶ 85-86. The commenters raise a number of objections to this conclusion.

1. Some of the commenters argue, as they have before, that information about which parties are connected to a multi-party call does not constitute "call-identifying information." For the most part, we have addressed these arguments in our prior filings, and we refer the Commission to our earlier discussion of this issue. As we have explained, CALEA defines "call-identifying information" to encompass information identifying "the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). A multi-party call can involve more than one "communication," as different parties join and leave the call; information about which parties are connected to the call identifies the "origin," direction," and "destination" of "each communication" within the call. See Government June Reply Comments at 52-53.

The commenters err by treating a multi-party, multi-leg call as a single "communication." A simple example suffices to show the shortcomings with this approach: assume that the subject is connected to two other people, A and B. The subject places A on hold and discusses a criminal matter with B. The subject then places B on hold and discusses an innocent matter with A. The

¹²(...continued)
associated with the subscriber's telephone number.

commenters are asking the Commission to treat the subject's criminal conversation with B and his entirely unrelated, innocent conversation with A as a single "communication." See, e.g., AT&T Comments at 9. Doing so would mean that law enforcement in many instances would lack proof of which party took part in the criminal conversation and which party did not. It would be manifestly contrary to the purposes of CALEA to construe the definition of "call-identifying information" in this fashion.

CTIA and Nextel argue that information about party joins, party holds, and party drops does not constitute "call-identifying information" because party join, hold, and drop messages "do not exist today." CTIA Comments at 25-26; Nextel Comments at 9; see also AT&T Comments at 9 (carriers do not "dynamically report any party's addition to or drop from a conference call") (emphasis added). This argument confuses the information available to the network and the messages used to encapsulate the information and convey it to law enforcement. As explained above, whether particular information exists in a network is relevant to a carrier's obligations under Section 103(a)(2); whether particular messages are already in existence to deliver that information to law enforcement is not. See pp. 27-28 supra.

US West asserts that party join information identifies the "origination" of a communication, not its "origin." US West Comments at 16. US West's distinction between "origination" and "origin" is, to be charitable, an elusive one. Far from being obviously distinct, the two words are often used interchangeably. See, e.g., Oxford English Dictionary, Compact Edition 2010 (1971) (definition of "origination" includes "origin"); Roget's International Thesaurus §§ 68.1, 153.5 (4th ed. 1977) (listing "origin" and "origination" as synonyms). Thus, saying that party join information

identifies the "origination" of the communication is tantamount to conceding that it identifies the communication's "origin."

US West also argues that party drop information does not identify the "termination" of a communication because "termination" refers to the connection that completes a circuit for a communication, not "the end of a call." US West Comments at 15-16. There is no indication that Congress meant to give "termination" the restrictive meaning assigned to it by US West.¹³ In any event, even if it were assumed that a party drop does not change the "termination" of a communication, party drop information nevertheless identifies the "direction" and "destination" of the communication that takes place after the dropped party leaves the call. When a subject who has been speaking to two other parties, A and B, continues to speak to A on the remaining call leg after B has dropped off the call, the direction and destination of the communication is different from what it was when the subject's words were being transmitted across two separate call legs to A and B.

Finally, US West and other commenters argue that the "origin, direction, destination, or termination" of a communication does not change when a party is placed on hold, so that party hold information does not come within the definition of "call-identifying information." See, e.g., US West Comments at 18; USTA Comments at 15. This argument fails for the same reason as does US West's argument about party drops. Like a party drop, a party hold changes the direction and

¹³ US West quotes a passage from the House Report that refers to the "originating and destination numbers of targeted communications." See US West Comments at 15-16 & n.44. This language makes no reference to "termination," and therefore offers no support for US West's reading of that term.

destination of the communications among the remaining parties; the only difference is that a party drop does so permanently, while a party hold does so temporarily.¹⁴

2. TIA asserts that the J-Standard's Change and Release messages convey substantially the same information that would be captured by the government's proposed party join and party drop messages. TIA Comments at 28-29. We have explained the shortcomings of the Change and Release messages in detail on several previous occasions; rather than repeat ourselves, we refer the Commission to our earlier discussions. See Government June Reply Comments at 51-52; Government December Comments at 46-47; see also Cutright Dec. § B.2.

AT&T asserts that industry "may have more efficient or effective ways than party messages to report joins and drops." AT&T Comments at 10. If so, industry is welcome to use them -- as long as they convey to law enforcement the same information about changes in party status, in the same timely manner, as the proposed party join and party drop messages would convey. However, we note that AT&T has not identified what these "more efficient or effective" alternatives might be. The Commission should not excuse carriers from providing party join and party drop messages without a specific explanation of alternative solutions and a concrete showing that the alternatives are equally effective.

3. BellSouth asks the Commission to rule that information about the parties to "meet me" conferences (see pp. 33-34 supra) is not "reasonably available" to switch-based CALEA carriers,

¹⁴ TIA makes the curious assertion that party hold information is "of no relevance to carriers." TIA Comments at 29 n.71. Far from being irrelevant, party hold information is vital for a carrier that is handling a multi-party call. See Cutright Dec. § B.2. If a carrier does not know when a party is placed on hold, the carrier cannot break the party's connection to the call, and if the carrier does not know when the party is taken off hold, the carrier cannot restore the connection.

because such information is "neither used nor generated by the switched network elements in the course of call processing to provide meet-me conference services." BellSouth Comments at 15. This comment assumes that the carrier is using a single intercept access point (IAP) located at the subscriber's switch and that the carrier would have to modify its network to deliver party information from the meet-me conference bridge to that switch. However, a carrier could deliver the party information to law enforcement directly from the network element providing the conference bridge service by adding appropriate IAPs there, eliminating the need to transmit the information from the bridge to the switch.

C. Subject-Initiated Dialing and Signaling Information

The Commission has tentatively concluded that information about a subject's use of flash hooks, feature keys, and similar subject-initiating dialing and signaling activity constitutes "call-identifying information," and that the J-Standard must be modified to require the delivery of such information when it is "reasonably available" to the carrier. Notice ¶¶ 91, 94. The commenters offer a variety of objections to this conclusion, most of which simply repeat arguments that were presented in previous rounds of comments and were rightly found unpersuasive by the Commission.

1. CTIA and PCIA argue that information about a subject's use of hold keys, flash keys, transfer keys, and conference keys does not constitute "call-identifying information." CTIA Comments at 29; PCIA Comments at 27-28. In making this argument, neither CTIA nor PCIA bothers to address the statutory definition of "call-identifying information": "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber" (47 U.S.C. § 1001(2)). As we have explained before, a subject's use of these feature keys changes the connections between the parties to the call, and in so

doing changes the "direction" and "destination" (and in some cases, the "origin" or "termination") of one or more "communication[s] generated or received" by the subject. Moreover, any use of feature keys or flash hooks by a subject to control a call constitutes "direction" of the communications by the subject.¹⁵ As a result, information about the use of these feature keys falls squarely within the definition of call-identifying information. See Government June Reply Comments at 46-48; Government December Comments at 49. Far from relying on a "Wonderland-like interpretation" (CTIA Comments at 29), the Commission's tentative conclusion is supported by a straightforward reading of the statutory definition.¹⁶

2. TIA and CTIA argue that the J-Standard's existing call event messages already provide substantially all of the call-identifying information that law enforcement would acquire through the reporting of subject-initiated dialing and signaling activity, and that the only additional information law enforcement would obtain through the reporting of this activity is "the actual keys pressed." TIA Comments at 30-31; CTIA Comments at 27. We have already addressed this argument in our earlier comments, and we refer the Commission to our prior discussion of this issue. As we have explained, it simply is not the case that the only additional information involved here is "the actual keys

¹⁵ Section 103 provides that a carrier's assistance capability obligations apply to all equipment, facilities, and services that "provide a customer or subscriber with the ability to originate, terminate, or direct communications * * * ." 47 U.S.C. § 1002(a) (emphasis added). The underscored language makes clear that, as used by Congress in Section 103, "direction" encompasses the activity of "directing" a communication, not just the path that the communication follows through the network.

¹⁶ Rather than parse the statutory definition of "call-identifying information," PCIA quotes selected excerpts from the discussion of call-identifying information in the House Report. See PCIA Comments at 27-28. The short response is that the meaning of "call-identifying information" is defined by the statute, not by the House Report. As noted above, the discussion in the House Report has serious limitations as a basis for interpreting the actual definition adopted by Congress. See pp. 22-23 supra.

pressed"; instead, the failure to report subject-initiated dialing and signaling activity will leave serious gaps in law enforcement's ability to understand the course of the subject's communications. See Government June Reply Comments at 48-49; Government December Comments at 49-50.

3. AirTouch and CTIA argue that the use of a feature key to initiate or disable call forwarding does not produce call-identifying information because it "does not directly result in the forwarding of a call," but rather identifies the number to which future calls will be directed. AirTouch Comments at 17; CTIA comments at 28. The definition of "call-identifying information," however, does not distinguish between calls in progress and impending calls. The use of a feature key to activate or deactivate call forwarding "identifies" the "destination" and "termination" of the "communication" to be forwarded, and therefore comes within the scope of CALEA's definition of "call-identifying information." We also note that if law enforcement is not notified that a subject has activated call forwarding at the time that the activation takes place, law enforcement may be unable to provision the surveillance adequately and may wind up losing call content which it is legally authorized to obtain.¹⁷

4. BellSouth suggests that the information that law enforcement would derive from a subject's dialing and signaling activity is redundant with the information that law enforcement would learn from party join, party hold, and party drop messages. See BellSouth Comments at 15-16. That is incorrect. Subject-initiated dialing and signaling activity may be either pre-cut-through or post-

¹⁷ A carrier may make call forwarding available as a usage-based feature, which a subscriber activates as needed by entering the appropriate access code (e.g., *72). Until the subscriber enters the access code, call forwarding is not part of his service package, and law enforcement therefore will not have had any reason to provision the surveillance to be able to intercept forwarded calls. If law enforcement receives immediate notification that call forwarding has been activated, it can act promptly to make the necessary changes in provisioning.

cut-through, and may be transmitted either in-band or out-of-band. Some of this activity may result in party joins, holds, or drops, but much of it will not. Conversely, there will be many instances in which a change in party connections does not reflect any subject-initiated dialing or signaling activity, such as when one of the other parties on a multi-party call hangs up. In short, while information about subject-initiated dialing and signaling activity may overlap with party join, hold, and drop information in some circumstances, the two categories of call-identifying information are by no means identical.

5. Finally, PCIA notes that, in some switches, the detection and collection of off-hook indicators occurs in a line module that is separate from the main processor of the switch. PCIA suggests that it may be onerous to redesign the switch to send this information from the line module to the main processor for delivery to law enforcement. PCIA Comments at 28. But the line module already must send the off-hook information to the main processor, so that the main processor can act on it in call processing. As a result, PCIA's stated fear about the modifications needed to report off-hook signals is considerably overstated.

D. In-Band and Out-of-Band Network Signaling

1. The J-Standard does not provide for the delivery of in-band and out-of-band network signals that identify call progress, such as busy signals, ringing, or call waiting tones. The Commission has tentatively concluded that delivery of certain kinds of in-band and out-of-band network signaling comes within a carrier's assistance capability obligations under Section 103 of CALEA, and has asked for comments regarding the scope of the obligation to deliver network signaling.

The industry comments reflect a persistent, and seemingly willful, misunderstanding of the scope of the network signaling that the government is seeking in this proceeding. First, we are asking a carrier to provide only those signals that are generated (or re-generated) by the carrier's own network. See Government Petition, Appendix 1, § 64.1708(d) ("in-band and out-of-band signaling from the subscriber's service"); Government June Reply Comments at 56-57. We are not asking a carrier to detect and report signaling that "is generated somewhere else and only 'passes through' a network element" of the carrier, as BellSouth suggests (BellSouth Comments at 17).¹⁸ Thus, it simply is not the case that the government's proposal will, for example, require carriers to develop and integrate miscellaneous tone detectors, as Ameritech suggests (Ameritech Comments at 9). A carrier does not need to use tone detectors to "detect" signals that the carrier itself is generating.¹⁹

Second, we are seeking only network signaling that results in signals that can be sensed by the subject. See Government Petition, Appendix 1, § 64.1708, Table 4. We have no interest in, and are not asking carriers to provide, any network signals that are not perceptible by the subject. For example, a cellular carrier would be under no obligation to provide law enforcement with the many out-of-band signaling messages that are "completely transparent to the user" (AirTouch Comments

¹⁸ CTIA is incorrect when it asserts that the government has departed from this position in the ESS process. CTIA Comments at 30. We have not asked for the delivery of any in-band or out-of-band network signaling that is not generated or regenerated by the carrier's own network.

¹⁹ TIA asserts that "literally hundreds of features supported by modern switches" involve the kind of in-band and out-of-band signaling sought by the government. TIA Comments at 33. But a variety of different features may employ the same in-band or out-of-band signal. As a result, the number of signals that carriers will be responsible for reporting will be considerably smaller than the number of features that give rise to those signals. See Cutright Dec. § B.4, n.8.

at 20), such as signaling messages used to control the cellular handset's power levels. Thus, the technical difficulties associated with providing access to such signals are simply irrelevant.

2. In our earlier filings, we have explained why the network signaling at issue here constitutes "call-identifying information." See Government June Reply Comments at 55-56. Several commenters take issue with us on this point, but their remarks largely repeat arguments to which we have already responded.

Nextel asserts that signaling from a carrier to a subject is not call-identifying information because it is not used to "route or process calls through [the] network." Nextel Comments at 13; PCIA Comments at 29. This argument reflects an astonishingly narrow view of what is involved in "process[ing] calls through [the] network." Without network signaling such as ringing, a subject simply will be unaware that an incoming call attempt is taking place, and the calling party will never reach the subject. Providing this kind of network signaling is an integral step in the carrier's processing of the call, not something unrelated to the task of call processing. Network signaling that reports the progress of outbound calls, such as busy signals, is likewise integral to the carrier's processing of such calls.

SBC asserts that audible network signals, such as ringing, constitute call content rather than call-identifying information, and that law enforcement can obtain such signaling only pursuant to a Title III order. SBC Comments at 14. SBC offers no legal support whatsoever for this radical theory, and none exists. Title III is designed to protect communications between the parties using a telecommunications network, not signaling by the network itself. Cf. 18 U.S.C. § 2510(8) (defining "content" of communications).

Several commenters assert that network notification of waiting voice mail messages (see Notice ¶ 93) is not covered by Section 103 of CALEA because voice mail is an "information service" (47 U.S.C. § 1001(6)) that is outside the scope of CALEA. See Ameritech Comments at 8; Nextel Comments at 14; US West Comments at 21. The commenters are correct that voice mail service is an "information service," and hence "[t]he storage of a message in a voice mail or E-mail 'box' is not covered" by CALEA. House Report at 23, reprinted in 1994 USCCAN at 3503 (emphasis added). But a telecommunications carrier may avail itself of this provision only "insofar as [it is] engaged in providing information services." 47 U.S.C. § 1001(8)(c)(i) (emphasis added). When a telecommunications carrier sends a network notification message to alert the subscriber that he has received a voice mail message, the carrier is acting in its capacity as a telecommunications carrier, not as an information service provider, and therefore the notification message remains within the scope of the carrier's assistance capability obligations.²⁰ In this respect, a message-waiting notification signal is no different from the "ping ring" notification that a carrier sends to a subscriber to alert him that an incoming call has been forwarded to another number. FBI Director Freeh's declaration explains the serious problems that lack of access to message-waiting signals causes for law enforcement. See Freeh Dec. ¶ 21(D).

3. Several commenters argue that the J-Standard already provides substantially all of the relevant call-identifying information that would be provided by the reporting of reasonably available in-band and out-of-band network signaling. TIA Comments at 34; PCIA Comments at 29-30;

²⁰ Bell Atlantic suggests that a voice mail notification message constitutes call content. See Bell Atlantic Comments at 10. That suggestion rests on the same logic as SBC's suggestion that all audible notification signals are call content, and it is wrong for the same reasons.

BellSouth Comments at 17. The commenters originally presented this argument in an earlier round of comments, and we have already answered it in detail in our own comments. See Government June Reply Comments at 57-59. For reasons set out there, there are many circumstances in which the J-Standard's existing messages, such as the TerminationAttempt message, will not provide law enforcement with knowledge of the network signaling presented to the subject.

E. Timing Requirements

1. Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication," and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(A)-(B). The Commission has tentatively concluded that, in order to satisfy this requirement, the J-Standard must be modified to require carriers to deliver call-identifying information within a "reasonable amount of time" and to "stamp" call-identifying information with the time of the underlying call event. Notice ¶ 104.

Several commenters, including TIA, claim that the J-Standard already obligates carriers to deliver call-identifying information "expeditiously." See, e.g., TIA Comments at 36. Unfortunately, however, it does not. When the J-Standard sets forth obligatory requirements, it uses mandatory language, such as "must" or "shall." See, e.g., J-STD-025, § 4.4 ("The IAP shall access the call-identifying information * * * unobtrusively") (emphasis added). The language in the J-Standard to which the commenters point, in contrast, simply states that "[t]he Call-Identifying Information IAP * * * provides expeditious access to the reasonably available call-identifying information * * * ." J-STD-025, § 4.4. This language is merely descriptive, not prescriptive; it describes the operation

of the call-identifying information IAP without purporting to impose any binding obligations regarding delivery time. A carrier therefore can comply with the J-Standard even if it does not deliver call-identifying information "expeditiously." If the J-Standard did implicitly require "expeditious" delivery of call-identifying information, then TIA presumably would have no objection if the Commission were to make that obligation explicit rather than implicit.

2. The government has proposed that call event messages be delivered within 3 seconds 99 percent of the time and that time stamps be accurate to within 100 milliseconds. Although the commenters stop short of endorsing these specific timing requirements, their comments generally acknowledge that timing values comparable to the ones proposed by the government are feasible. See, e.g., TIA Comments at 36-37.

Several commenters suggest that industry and law enforcement have reached a working consensus regarding timing requirements through the ESS process. See, e.g., BellSouth Comments at 18; CTIA Comments at 31. In its current form, the ESS draft document sets forth separate timing requirements for each call-identifying information message, most but not all of which call for delivery within 3 seconds, and the draft further provides that time stamps shall be precise to within 100 milliseconds. See PN-4177 Working Document Revision 12, §§ 4.2.5.1, 4.2.5.2. These proposed values strongly confirm the feasibility of our own proposed timing requirements. However, the Commission should be aware that the ESS document is a working draft that has not been balloted, and the timing provisions in the document are subject to change. As a more general matter, the Commission should also be aware that the ESS process itself has come under attack by industry in recent weeks -- a development that we discuss further below in connection with the Commission's proposal to leave the drafting of revised standards to TIA. See p. 75 infra. As a

result, the Commission should not reach the mistaken conclusion that "consensus" between industry and law enforcement about timing issues has eliminated the need for Commission action.

3. The industry comments raise several specific technical questions relating to the timing requirements proposed by the government. First, AirTouch and SBC suggest that it will be difficult, if not impossible, to ensure that time stamps are synchronized throughout a carrier's network. See AirTouch Comments at 21; SBC Comments at 15. As we have made clear in our previous comments, however, we are not asking for this kind of synchronization. See Government June Reply Comments at 65-66. As a result, its feasibility is irrelevant.

Second, SBC suggests that imposing "strict" time stamping requirements could lead to a loss of call content. SBC Comments at 15. This suggestion is simply incorrect. Neither the application of a time stamp to a call event message nor the precision of the time stamp has any effect on the delivery of call content. Conventional switches are capable of setting up roughly 360,000 calls per hour and can begin transmitting a message within 10 microseconds. Given these speeds, the process of adding a time stamp to call event messages will not prevent a switch from performing call setup tasks in a timely manner. See Cutright Dec. § B.8.

Third, AT&T suggests that the 3-second delivery requirement should apply to "the first bit of a timing message measured at the point of demarcation between the carrier network and law enforcement's collection facilities." AT&T Comments at 15. We have no objection to this suggestion. The carrier is not responsible for any delays in delivery beyond the demarcation point; as long as the message is delivered to the demarcation point within 3 seconds, the delivery time beyond that point is law enforcement's responsibility.

4. AirTouch (at 21) and SBC (at 15) assert that the adoption of specific timing requirements by the Commission would violate Section 103(b)(1)(A) of CALEA, which provides that CALEA "does not authorize any law enforcement agency or officer * * * to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service * * * ." 47 U.S.C. § 1002(b)(1)(A). It is doubtful whether this provision applies to the Commission's actions in this proceeding, since the Commission is not conventionally regarded as a "law enforcement agency." In any event, the Commission is not being asked to "require any specific design of equipment, facilities, services, features, or system configurations * * * ." The timing requirements suggested by the government constitute a performance standard, not a design standard; the Commission is not being called on to prescribe "any specific design" by which the timing requirements are to be met. Finally, the Commission's modifications to the J-Standard, like the J-Standard itself, will constitute a voluntary standard that carriers are not obligated to follow if they are able to satisfy the underlying requirements of Section 103 by other means. See Government May Comments at 14-15. As a result, the Commission will not be, in the language of Section 103(b)(1)(A), "requiring" anything by adding specific timing provisions to the J-Standard.

F. Surveillance Integrity

The government has asked the Commission to modify the J-Standard to incorporate several capabilities relating to surveillance integrity. The Commission has tentatively concluded that these capabilities are not required by Section 103 of CALEA. In our most recent comments, we have asked the Commission to revisit that conclusion. See Government December Comments at 58-66. As we explained there, whether or not CALEA requires the specific surveillance integrity measures

proposed in the government's rulemaking petition, it manifestly imposes a general obligation on the part of carriers to take affirmative steps to ensure the integrity of ongoing surveillance, and the J-Standard is deficient because it excuses carriers from taking any such steps.

Because the Commission has tentatively declined to add the proposed surveillance integrity capabilities to the J-Standard, the other commenters devote relatively little attention to them. Nevertheless, the commenters do make several points that call for a response.

1. PCIA and TIA argue that implementing automated surveillance status messages would require wireless carriers to engage in a fundamental redesign of their networks, because wireless networks are not currently configured to poll remote switches to ensure that they are operational and properly configured for surveillance purposes. PCIA Comments at 19; TIA Comments at 38. This argument rests on the assumption that the reporting of surveillance status messages would require a centralized implementation. But rather than polling each network element from a centralized location, a wireless carrier would be free to transmit surveillance status messages directly from each network element involved in the surveillance, just as each switch will separately transmit call-identifying information and call content to law enforcement. Redesigning the network to provide for centralized polling would not be required; the choice between a centralized approach and a decentralized one is left to the carriers and their vendors. See Cutright Dec. § B.5.

US West suggests that automated surveillance status reporting is unnecessary because law enforcement, not the carrier, "typically" is "the first to become aware of any problem with a wiretap." US West Comments at 22. What US West overlooks is that as electronic surveillance migrates from the local loop to the switch, it becomes far more difficult for law enforcement to "become aware" of a problem in the first place. That is, indeed, the very reason why we have asked for the delivery

of surveillance status messages. When law enforcement carries out traditional electronic surveillance over the local loop, it has physical access to the subscriber's line and can confirm for itself that the surveillance is operating and is directed at the right subscriber. See Yarbrough Dec.

¶ 43. When surveillance becomes switch-based, law enforcement no longer has physical access to the interception site and loses its former capability to determine directly the status of the surveillance. Thus, under CALEA, law enforcement must rely on the carrier to take affirmative steps -- either by automated surveillance status reporting or by some other means -- to ensure that the surveillance is operating properly. *Id.* ¶¶ 44, 47. In the context of cellular communications, law enforcement has already experienced losses of authorized surveillance information because of the failure of carriers to take such steps.

2. PCIA asserts that delivery of an automated continuity check would require carriers to install C-tone generators at the switch level. PCIA Comments at 20. That is incorrect. A C-tone is one form of continuity check, but it is not the only form that would be acceptable. As we have explained before, we have no objection to the use of existing tones or idle patterns, and we would accept the use of any tones or patterns already in use by the network that could match the functionality of the continuity check described in the government's rulemaking petition. See Government June Reply Comments at 69.

3. PCIA asserts that implementation of an automated feature status message would be infeasible because carriers "do not maintain a real-time database of which features have been implemented by which subscriber at any given time." PCIA Comments at 21. If this were true, it is hard to understand how a carrier could provide service to its subscribers. When a subscriber attempts to invoke a particular feature, such as call forwarding or three-way calling, the network's

first task is to determine -- in real time -- whether the feature is available to the subscriber. See Cutright Dec. § B.5. The proposed feature status message therefore does not require the network to detect and report feature status information that is not already available to the network.

G. Post-Cut-Through Dialing

1. One of the principal deficiencies in the J-Standard is its failure to require originating carriers to deliver digits that are dialed by the calling party "post-cut-through" to reach the person with whom the calling party wishes to speak. The Commission has tentatively concluded that "post-cut-through digits representing all telephone numbers needed to route a call * * * are call-identifying information," and therefore must be provided to law enforcement when they are reasonably available to the carrier. Notice ¶ 128. For reasons that we have set forth previously, this conclusion is correct. See Government June Reply Comments at 38-41; Government December Comments at 66-67. Nevertheless, many commenters take issue with it.

The commenters' principal argument is that post-cut-through dialed digits do not constitute call-identifying information "for," or "with respect to," originating carriers. We have already addressed this argument above, in connection with our general discussion of the obligation to provide access to call-identifying information. As explained above, the statutory definition of "call-identifying information" encompasses all dialing and signaling information that "identifies the * * * destination" of "each communication generated or received by a subscriber" (47 U.S.C. § 1001(2)), regardless of whether the particular carrier from whom the information is being sought uses the information for call routing purposes. As a result, the fact that an originating carrier does not use

post-cut-through digits to route the call through its network is simply irrelevant. See pp. 23-25 supra.²¹

Nextel argues that "call-identifying information pertains only to 'the equipment, facilities, or services of a subscriber of such carrier,' not to subsequent LECs or IXC's." Nextel Comments at 18 (emphasis in original). But the language that Nextel is quoting comes not from Section 103(a)(2), the assistance capability provision governing call-identifying information, but instead from Section 103(a)(1), the provision concerning delivery of call content. Moreover, Section 103(a)(1) itself sweeps more broadly than Nextel tries to suggest. It encompasses "all wire and electronic communications" carried by a carrier to or from its subscribers' equipment, facilities, or services (47 U.S.C. § 1002(a)(1) (emphasis added)), and therefore unquestionably includes communications between a subscriber and a called party after the cut-through takes place.²² As a result, even if a carrier's obligation to deliver call-identifying information under Section 103(a)(2) were expressly confined to information about communications covered by Section 103(a)(1) (and it is not), that obligation would still encompass the post-cut-through digits dialed by the subscriber to reach the called party.

²¹ For this reason, it is immaterial that cellular and PCS systems do not use DTMF audio digits for call routing purposes, as AirTouch argues. See AirTouch Comments at 25-26. If a cellular or PCS subscriber engages in post-cut-through dialing on a mobile handset to complete a call, the dialed digits constitute "call-identifying information" regardless of how the cellular or PCS carrier treats the digits, because they "identify the * * * destination" of a "communication generated or received by [the] subscriber."

²² As the Commission has noted in other settings, "a 'completed' call is a call that is answered by the called party." Report and Order, In re Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, Docket No. 96-388 (released Sept. 20, 1996), at 33. Thus, when a subscriber calls another party by using an "800" long-distance service, the subscriber's call is not completed until it reaches the called party.

EPIC suggests that if post-cut-through dialed digits constitute "call-identifying information," as the government contends, then so would the words spoken by a subject who orally gives a telephone number to a long-distance operator. EPIC Comments at 32. This reductio ad absurdum is incorrect. The definition of call-identifying information is confined to "dialing or signaling information" (47 U.S.C. § 1001(2) (emphasis added)), and words spoken by one person to another do not constitute "dialing or signaling information."²³

2. EPIC, along with other commenters, points out that a subject may engage in post-cut-through dialing for purposes other than call completion, such as sending instructions to an automated bank account or entering a credit card number. EPIC Comments at 28. EPIC argues that post-cut-through digits entered for such purposes do not constitute call-identifying information. We agree. Contrary to EPIC's claim, we are not trying to stretch the definition of "call-identifying information" to encompass post-cut-through dialing that is used for purposes other than call routing. See Government June Reply Comments at 39. Our position is simply that when post-cut-through dialing is performed in order to complete a call, it constitutes call-identifying information, and it therefore comes within the scope of the carrier's obligations under Section 103(a)(2) of CALEA.²⁴ In these

²³ This does not imply that law enforcement would necessarily have to obtain a Title III interception order to obtain access to phone numbers conveyed orally to an operator. See Smith v. Maryland, 442 U.S. 735, 744 (1978) (indicating that subject who "placed his calls through an operator" would have "no legitimate expectation of privacy" in the words spoken to the operator).

²⁴ EPIC quotes from a letter from the Department of Justice to Congress regarding proposed "clone pager" legislation. The letter, a copy of which is attached to EPIC's comments, states that "the information transmitted [to a pager] after a phone call is connected to the called party" is "substantive in nature," because it is "not used to direct or process the call, but instead [to] convey certain messages to the recipient." Letter from Acting Assistant Attorney General Ann M. Harkins to the Hon. Henry J. Hyde, May 20, 1998, pp. 2-3 (emphasis added). As the underscored language
(continued...)

circumstances, the only real issue is how to meet law enforcement's minimization obligations, not whether law enforcement should be provided with access to the information in the first place.

If a carrier has the technical capability to distinguish automatically between post-cut-through digits used for call completion and post-cut-through digits entered for other purposes, the carrier is free to employ that capability to give law enforcement only the digits used in call completion. To our knowledge, however, no such technical capability currently exists. See Government December Comments at 67. In the absence of such a capability, the carrier must deliver either all post-cut-through digits or none, and the latter course is inconsistent with the carrier's obligation to provide call-identifying information under Section 103(a)(2). For reasons that we have explained before, nothing in CALEA excuses a carrier from delivering post-cut-through digits that are "call-identifying information" simply because doing so will unavoidably result in the delivery of other post-cut-through digits that are not. See Government June Reply Comments at 40-41.

EPIC suggests that when law enforcement receives post-cut-through digits that are not dialed for call routing purposes, it is engaging in an "interception" of communication for purposes of Title III, and therefore must make the heightened showing required to obtain a Title III interception order, rather than relying on a pen register order. See EPIC Comments at 28-29. This argument is incorrect. Congress placed the use of pen registers and trap-and-trace devices outside the scope of Title III altogether. See 18 U.S.C. § 2511(h)(i); see also Smith v. Maryland, 442 U.S. 735 (1979). The pen register statute authorizes law enforcement to acquire all "numbers dialed or otherwise

²⁴(...continued)

makes clear, the legal analysis in the Department's letter in no way suggests that dialing activity that takes place before "a call is connected to the called party," for the purpose of "direct[ing] or process[ing] the call," is substantive in nature.

transmitted" by the subject using the monitored facilities (18 U.S.C. § 3127(3)); it does not restrict that authorization to numbers dialed for call processing purposes. Thus, at least as long as a carrier is unable to differentiate between digits dialed for call processing purposes and digits dialed for other purposes, law enforcement may obtain all dialed digits from the carrier pursuant to a pen register order without running afoul of Title III. If the law were otherwise, there would have been no reason for Congress to enact 18 U.S.C. § 3121(c), the pen register statute's minimization provision, which obligates law enforcement to "use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." This provision presupposes that law enforcement agencies executing pen register orders can and will receive dialing and signaling information that is not "utilized in call processing," and simply directs that such information not be "record[ed] or decod[ed]" if (and only if) reasonably available technology so permits.²⁵

In a similar vein, several commenters suggest that carriers who provide law enforcement with access to post-cut-through dialed digits might be exposed to legal liability for doing so. See, e.g., Nextel Comments at 20. This suggestion is thoroughly misconceived. Title III expressly states that providers of wire and electronic communication services "are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance," whenever they are provided with an

²⁵ AT&T asserts that "[t]here are no provisions in the pen register statute that require minimization." AT&T Comments at 21; Nextel Comments at 20 n.47 (same). This assertion simply overlooks 18 U.S.C. § 3121(c). See House Report at 17, reprinted in 1994 USCCAN at 3497 (CALEA "requires law enforcement to use reasonably available technology to minimize information obtained through pen registers").

appropriate court order. 18 U.S.C. § 2511(2)(a)(ii). Title III further states that "[n]o cause of action shall lie in any court" against a provider of wire or electronic communications services "for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter." Ibid. The pen register statute likewise states that "[n]o cause of action shall lie in any court" against a provider of wire or electronic communication services "for providing information, facilities, or assistance in accordance with the terms of a court order" under the pen register statute. Id. § 3124(d). Finally, Title III and the pen register statute both provide that "good faith reliance" on a court order or other legal authorization is "a complete defense against any civil or criminal action" brought under Title III, the pen register statute, or any other law. Id. §§ 2520(d)(1), 3124(e). As a result, a carrier that complies with an appropriate court order requiring the carrier to provide access to post-cut-through dialed digits faces no risk of legal liability.

3. TIA and several other commenters argue that law enforcement should not look to the originating carrier for post-cut-through dialed digits, but rather should turn to the carrier that uses the post-cut-through digits to route the call. TIA suggests that if post-cut-through digits can be obtained from other carriers, requiring originating carriers to provide them would be inconsistent with Section 107(b)(1)'s mandate to use "cost-effective methods" for meeting CALEA's assistance capability requirements. TIA Comments at 42.

Unfortunately, the alternative of obtaining post-cut-through digits from other carriers is an illusory one. For reasons that we have discussed at length in our earlier filings, post-cut-through digits cannot be obtained "expeditiously" from other carriers (see 47 U.S.C. § 1002(a)(2)), and often will not be available at all. See Government June Reply Comments at 41-42 & n.24; Government December Comments at 68-69. As a result, law enforcement's request for post-cut-through digits

from originating carriers is not a prohibited demand for "one-stop shopping," as the commenters repeatedly suggest (e.g., Bell Atlantic Comments at 10). Instead, it is a matter of practical necessity.

Ameritech and BellSouth suggest that, rather than requiring the originating carrier to detect post-cut-through digits and extract them for delivery on a call data channel (CDC), law enforcement agencies should provision a call content channel (CCC) from the originating carrier's switch and extract the DTMF tones at the collection facility. See Ameritech Comments at 12; BellSouth Comments at 18. Under this proposal, the originating carrier would transmit to law enforcement not only the post-cut-through dialed digits, but also the content of the subject's post-cut-through communications. Ameritech and BellSouth suggest that this approach would be more economical than requiring carriers to modify their equipment to detect post-cut-through dialing.

Apart from the fact that the J-Standard currently does not require the delivery of post-cut-through digits by any means, including delivery over a CCC, there are at least two major problems with this proposal. First, while Ameritech and BellSouth (and other commenters) express concern about the cost of dialed digit extraction for originating carriers, they take no account of the costs associated with requiring law enforcement to provision CCCs to capture post-cut-through dialing in pen register cases. If post-cut-through digits are extracted by the originating carrier, they can be delivered over the same CDC that is being used to implement the pen register order. But under Ameritech's and BellSouth's proposal, law enforcement would also have to provision at least one CCC in addition to the CDC, and law enforcement would have to do so in every pen register case simply to ensure that it is capable of identifying the parties that the subject is calling.

When law enforcement leases a dedicated line, it typically has to pay an initial setup charge of roughly \$700 and an additional payment of \$100 per month, although higher prices are not

uncommon. This means a cost of roughly \$1,000 for a pen register surveillance that lasts three months, a common length of time. In a typical year, the FBI executes pen register and trap-and-trace orders on approximately 10,000 lines, and state and local law enforcement agencies perform a comparable volume of pen register and trap-and-trace surveillance. Thus, the cost entailed in provisioning CCCs for pen register cases could amount to as much as \$20 million per year -- each year, year after year. It is understandable that Ameritech and BellSouth do not dwell on these costs, since they represent a source of revenue rather than expense to carriers. But to the extent that the Commission deems cost considerations to be relevant under Section 107(b), the substantial costs of requiring law enforcement to provision CCCs for pen register cases should weigh against this proposal.

Second, as we have pointed out previously, delivering the contents of a subject's post-cut-through communications to law enforcement pursuant to a pen register order poses unnecessary risks to privacy interests. See Government June Reply Comments at 45. We do not mean to suggest, as some commenters do, that the arrangement proposed by Ameritech and BellSouth would exceed the scope of law enforcement's authority under the pen register statute and could be implemented only pursuant to a Title III order. Nevertheless, it would create a risk that innocent conversations might be heard inadvertently by law enforcement in the course of pen register surveillance. Where it is practical for a carrier to deliver dialing and signaling information to law enforcement without also delivering the contents of the communication, the Commission may take account of privacy concerns in selecting among the alternatives. See 47 U.S.C. § 1006(b)(2).

4. In earlier filings, we have discussed the mechanics of detecting and extracting post-cut-through dialed digits. See Government June Reply Comments at 43; Government December

Comments at 67. We have only two points to add in response to the comments of the other parties on this issue. First, the detection of post-cut-through digits does not have to take place inside the switch; it can be performed outside the switch by means of a "loop around" arrangement, and doing so may be both easier and less expensive. See Cutright Dec. § B.7. Second, some wireless switches generate DTMF tones in response to out-of-band messages originating at the wireless handset. Carriers using these switches have no need to install tone decoders at the switch and send the generated tones to law enforcement; instead, they simply can report the messages that cause the switch to generate the tones.

H. Location Information

In certain circumstances, the J-Standard requires carriers to provide law enforcement agencies with location information at the beginning and end of communications to and from mobile terminals. The Commission has tentatively concluded that the location information prescribed by the J-Standard is "call-identifying information" under CALEA. Notice ¶ 52. CDT takes issue with that tentative conclusion and urges the Commission to remove the location information provisions from the J-Standard. See CDT Comments at 4-12.

In large measure, CDT's arguments about location information reprise CDT's earlier comments in this proceeding. We have addressed those comments in detail in our own previous filings, and we refer the Commission to our earlier discussions for an explanation of the shortcomings in CDT's legal argument. See Government May Comments at 17-21; Government June Reply Comments at 78-79. Nevertheless, several points in CDT's most recent filing call for a further response.

At the outset, it is critical for the Commission to keep in mind that the J-Standard provides for the delivery of location information only when law enforcement has legal authority to obtain such information. Location information is included in J-Standard messages only when "delivery is [legally] authorized." See, e.g., J-STD-025, § 5.4.1, Table 1 (Location parameter, Usage column); see also id. § 5.4 (discussing meaning of "conditional" parameters). The J-Standard does not require the delivery of location information unless law enforcement is acquiring such information pursuant to an appropriate court order or other legal authorization. As a result, the J-Standard creates no risk whatsoever that law enforcement will obtain location information that Congress does not want it to obtain.

CDT nevertheless argues at length that the Commission's tentative conclusion conflicts with "one of the key compromises struck in 1994 when CALEA was being drafted and debated." CDT Comments at 2. This gets the matter exactly backward. CALEA indeed embodies a compromise regarding location information. But it is CDT, not the Commission, that has misunderstood the nature of the compromise.

The legislative compromise regarding location information is written into Section 103(a)(2) of CALEA, in plain and unambiguous terms: "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices * * * , * * * call-identifying information shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2) (emphasis added). Congress could hardly have been any clearer about its intent: when law enforcement is proceeding "solely pursuant to the [legal] authority for pen registers and trap and trace devices," carriers are not to treat location information as call-identifying information, but when law enforcement has been duly authorized to acquire location information

under other electronic surveillance statutes, location information remains part of call-identifying information.²⁶ The J-Standard is consistent with this intent; CDT's position is not. See Government May Comments at 18-19.

CDT argues that location information does not come within the scope of call-identifying information because the statutory definition of call-identifying information does not include the term "location." CDT Comments at 5. But the definition does include the terms "origin" and "destination," and as the Commission has noted, those terms readily encompass the location from which a wireless call is being sent or received. See Notice ¶ 52. It may well be true, as CDT says, that "origin" and "destination" have further meanings in addition to location (CDT Comments at 5), but it hardly follows that their meanings exclude location. See, e.g., Oxford English Dictionary, Compact Edition 702 (1971) ("destination" means, inter alia, "the place for which a person or thing is destined"); id. at 2010 (giving examples of the use of "origin" to signify location). Moreover, if "origin" and "destination" are read to exclude location information altogether, as CDT urges, then the location proviso in Section 103(a)(2) becomes superfluous, CDT's claims to the contrary notwithstanding.

It is not the case, as CDT suggests, that the Commission's reading of "origin" and "destination" gives those terms different meanings for wireless and wireline communications. The

²⁶ US West asserts that the pen register statute is the only legal basis for acquiring location information, and hence the location proviso of Section 103(a)(2) serves to place location information entirely beyond the reach of law enforcement. US West at 25. That assertion is incorrect. There are at least two other sources of legal authority under which law enforcement may, upon a proper showing, obtain location information: an interception order under Title III, 18 U.S.C. §§ 2510 et seq., and an order for the disclosure of customer records under 18 U.S.C. § 2703(c)-(d). CDT, unlike US West, makes no claim that the pen register statute is the sole source of authority for this information.

terms encompass location both in the wireless setting and the wireline setting. In the case of wireline communications, however, the fixed location of the subscriber's terminal means that the number of the party using the terminal identifies the location of the call, so no separate location information is required.²⁷

Finally, CDT conspicuously fails to explain why Congress would have intended to exclude location information from the scope of CALEA altogether, even in circumstances where it is uncontested that law enforcement has full legal authority to obtain such information. CDT argues that information about the location of a wireless handset is more invasive than information about the location of a wireline terminal because the user of a wireless handset "almost always is the individual subscriber" (CDT Comments at 12), so that law enforcement learns not only where the call is coming from but also who is speaking. CDT's assumptions about who uses wireless handsets are debatable: wireless handsets may be used by many persons other than individual subscribers, such as a subscriber's family members and colleagues, and in the case of corporate usage (which accounts for a substantial share of wireless traffic), the user could be any one of hundreds or even thousands of a corporate subscriber's employees. In any event, CDT's real argument here is not with the Commission but with Congress, for the J-Standard provides access to location information only when laws other than CALEA authorize law enforcement to obtain such information. To the extent that CDT has concerns about the privacy implications of those laws, its recourse lies outside the confines of this proceeding.

²⁷ CDT asserts that the Commission's reading of "origin" and "destination" does not explain why the J-Standard provides location information at the end of an outgoing call. CDT Comments at 6. The explanation is that the location of the mobile handset identifies the "origin" of the communication regardless of whether the communication is beginning or ending.

I. Packet Mode Communications

1. From the outset of this rulemaking proceeding, CDT has taken issue with Section 4.5.2 of the J-Standard, which permits carriers transmitting packet mode communications to send law enforcement the entire packet data stream associated with a given communication, including the content of the communication as well as the associated call-identifying information in the packet header. See J-STD-025 § 4.5.2, ¶ 2 (Packet Data IAP). In our earlier comments, we have explained why this provision of the J-Standard is consistent with the assistance capability requirements of CALEA. See Government May Comments at 21-22; Government December Comments at 77-80. As we have explained, in pen register cases, 18 U.S.C. § 3121(c) obligates law enforcement to "use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Technology is currently available to law enforcement that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for "recording or decoding." The J-Standard relies on law enforcement to comply with its legal obligations under 18 U.S.C. § 3121(c) in this fashion, and nothing in Section 103(a) -- or any other provision of CALEA -- prohibits this arrangement.

In its latest comments, CDT elaborates on its proposed alternative to the J-Standard's current packet data delivery provision. CDT argues that Section 103(a)(2) of CALEA obligates a carrier only to provide law enforcement with the information in a packet that the carrier itself uses to route the communication, and that the carrier is under no obligation to deliver information in the packet that is used for routing purposes by other carriers who are "upstream" or "downstream" in the data transmission path. CDT proposes that "any carrier using packet technologies should disclose

pursuant to a pen register order the transactional information that it uses to process communications," and should not be required to provide "the transactional information used by other carriers." Id. at 13 (emphasis in original). Thus, when a packet is transmitted across the networks of (for example) four different carriers, law enforcement should (under CDT's proposal) ask each carrier separately for the information in the packet header that that carrier uses in routing the communication.

This proposal has profound problems, both legally and practically. If the Commission were to adopt it, law enforcement's electronic surveillance capabilities in cases involving packet mode communications would be severely compromised.

We have already identified the basic legal shortcoming of CDT's position in connection with our general discussion of call-identifying information. See pp. 23-25 supra. As we explained there, CDT's position rests on the proposition that "call-identifying information" is a "subjective" or "relative" concept, meaning that the status of information as "call-identifying information" depends on the use to which a particular carrier puts it. Under this view, information changes back and forth from call-identifying information to call content as it passes between a carrier that uses it for call routing purposes and a carrier that does not. See CDT Comments at 21-22.

The problem with this argument is that, as we have explained above, it simply cannot be squared with CALEA's definition of "call-identifying information." Particular information in a packet header either does or does not "identif[y] the origin, direction, destination, or termination" of a "communication generated or received by [the] subscriber." 47 U.S.C. § 1001(2). If it does,

it is "call-identifying information" -- period. It does not flicker back and forth spectrally from one state to another, like Marley's ghost.²⁸

Not only is CDT's position legally unsupportable, but it presents fundamental practical problems as well. CDT's proposal would require law enforcement to seek information from every carrier in the packet data stream in order to determine the origin and destination of a single packet mode communication. In many instances, law enforcement would have no way of knowing in advance which "downstream" carriers would wind up handling the communication after the packet stream passes through the hands of the originating carrier. Law enforcement therefore would be unable to identify the destination of an outgoing communication at the time that it takes place, and would never be able to identify the destination if, as ordinarily will be the case, the downstream carrier does not retain a record of the call-identifying information in the packet header after the communication is complete.

Moreover, in many instances, CDT's proposal would require law enforcement to serve pen register orders on Internet service providers (ISPs). See CDT Comments at 16. To the extent that ISPs are engaged in providing "information services" (47 U.S.C. § 1001(6), (8)(c)(i)), they are outside the scope of CALEA's assistance capability requirements. See House Report at 18, reprinted in 1994 USCCAN at 3498. Thus, the effect of CDT's proposal -- and, it is fair to assume, CDT's underlying purpose -- is to diminish law enforcement's access to call-identifying information that it is legally authorized to acquire, by forcing law enforcement to turn from telecommunications

²⁸ "Scrooge, having his key in the lock of the door, saw in the knocker, without its undergoing any intermediate process of change -- not a knocker, but Marley's face. * * * As Scrooge looked fixedly at this phenomenon, it was a knocker again." Charles Dickens, A Christmas Carol 23 (1991 ed.).

carriers who are subject to CALEA's assistance capability requirements to information service providers who are not.

The fundamental object of CALEA is to narrow the gap between law enforcement's legal authority to conduct electronic surveillance and its technical capability to exercise that authority. CDT's proposal would have precisely the opposite effect: it would expand that gap rather than narrow it. CDT's proposal thus strikes at the heart of Congress's goals in enacting CALEA. The Commission must not permit Congress's objectives to be undermined in this fashion.

2. Bell Atlantic Mobile urges the Commission "to declare as part of any capability rule that the rule does not apply to packet transmissions," such as those handled by Bell Atlantic Mobile's Cellular Digital Packet Data network. Bell Atlantic Mobile Comments at 12. This suggestion is misconceived. As explained in our prior comments, CALEA does not distinguish between packet mode and circuit mode communications. See Government December Comments at 81-82. The assistance capability requirements of Section 103(a) of CALEA apply to all "telecommunications carriers" and encompass all "wire and electronic communications" carried by such carriers. 47 U.S.C. § 1002(a)(1)-(2). If a telecommunications carrier is transmitting a "wire communication" or an "electronic communication," as those terms are defined (18 U.S.C. § 2510(1), (12)), the carrier must comply with Section 103 with respect to those communications, regardless of whether the carrier is using packet mode technology or some other technology to transit the communications. Like CALEA itself, the J-Standard encompasses packet mode as well as circuit mode communications, and the Commission's final Report and Order should do likewise.

3. Metricom argues that carriers should not be required to provide law enforcement with access to wireless packet-mode data, because such data are typically encrypted by users in ways that,

according to Metricom, "make meaningful interception of call content impossible." Metricom Comments at 2-4. The short answer to this argument is that CALEA does not relieve carriers from their obligation to provide access to call content (47 U.S.C. § 1002(a)(1)) when a communication is encrypted. Instead, CALEA provides that "[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002(b)(3). As this provision indicates, Congress was well aware that particular communications might be encrypted. Its response was assign responsibility for decryption to law enforcement, not to release carriers from the duty to deliver encrypted communications to law enforcement in the first instance.

III. Comments Regarding Implementation Issues

A. Revision of J-Standard

1. In our earlier comments, we addressed the Commission's proposal to assign the TIA standard-setting committee responsible for the J-Standard with the task of preparing new technical standards that correct the deficiencies in the J-Standard identified by the Commission. See Government December Comments at 30-34. In some respects, the comments submitted by the other commenters make the same points that we have made, such as the importance of giving TIA precise "marching orders" in order to minimize confusion and disagreement about its goals. In other respects, however, the commenters have a different view about the course that a remand should follow.

The principal disagreement concerns how long the process of revising the J-Standard should take. The Commission's Notice proposes that TIA "complete any such modifications * * * within

180 days of release of the Report and Order in this proceeding." Notice ¶ 133. We endorse that timetable. However, TIA argues that it will take 180 days simply to prepare draft standards for balloting, and that an additional 3 to 5 months should be permitted for the balloting process. TIA Comments at 3, 13, 15. TIA thus asks the Commission to allow as much as 11 months for redrafting the J-Standard, and other commenters ask for even more time. See, e.g., US West Comments at 30-31 (14 to 17 months).

We urge the Commission to adhere to its proposal that the revision process be completed within 180 days, not simply to provide for the commencement of balloting within that time. TIA's proposed timetable reflects a "business as usual" approach, in which committee meetings are scheduled on a relatively infrequent and episodic basis. If the Commission intends to enlist the aid of industry in revising the J-Standard, rather than performing that task itself, TIA's business-as-usual approach must give way to the need to implement CALEA's assistance capability requirements as soon as possible. Congress's goal of preserving law enforcement's ability to carry out legally authorized surveillance should not be undermined by further delays in the implementation process.

If the Commission is specific about the changes required in the J-Standard, there is no reason why the parties cannot produce a ballot-ready draft within 90 days, which would allow an additional 90 days if necessary for balloting and post-ballot revisions. As noted in our prior comments, law enforcement and industry have been engaged in ongoing discussions for the past year, under the aegis of TR45.2's ESS (Enhanced Surveillance Services) project, about technical standards that would implement the capabilities at issue in this proceeding. As a result of that process, TIA would not be starting from scratch, but rather could draw on the substantial efforts and progress already made in defining the added assistance capabilities.

In recent weeks, industry has threatened to terminate the ESS project, while suggesting that law enforcement rather than industry is responsible for the failure to complete the process. The timing of industry's action, coming when the Commission is deciding how much time will be required to revise the J-Standard, strongly suggests that industry is trying to minimize the progress already made by the ESS project in order to justify a longer "remand" period. The government has made clear to industry that we strongly support the work produced by the ESS project. If industry nevertheless chooses, for its own reasons, to discontinue the ESS project, the Commission should not allow industry to reap the benefits by extending the time for implementing the Commission's decision and order. Indeed, if industry is serious about abandoning the ESS project, the Commission may well need to reconsider whether TIA should be entrusted at all with the task of implementing the Commission's changes to the J-Standard.

Industry's threat to walk away from the ESS process also underscores the need for the Commission to monitor the remand process to ensure that TIA meets the deadlines set by the Commission. In addition to designating Commission staff members to attend the standards meetings as observers (Government December Comments at 33-34), the Commission may also wish to require periodic status reports from TIA. If the Commission sees that its deadlines are not going to be met, it should accept proposed technical standards from law enforcement as a basis for further proceedings before the Commission. See Government December Comments at 33.

B. Compliance Deadline

1. The other major issue relating to implementation is the deadline for compliance with the assistance capabilities that the Commission adds to the J-Standard. In our comments, we suggested that the Commission require compliance no later than 18 months after the revisions to the J-Standard

are complete. If the revision process takes 180 days, that would mean a compliance deadline of 24 months after the Commission's report and order. See Government December Comments at 29-30. Thus, if the Commission were to issue its report and order in the second quarter of 1999, compliance would be required by the second quarter of 2001.

Predictably, most (although not all) of the industry commenters argue for a far later compliance deadline. TIA suggests that compliance with the added capability requirements be deferred until June 2003 -- more than four years from now. TIA Comments at 2, 18. Other commenters propose similarly extended compliance deadlines. See, e.g., AirTouch Comments at 28; GTE Comments at 14-15.

TIA suggests that a prolonged implementation timetable is necessary because most manufacturers "will not be able to begin their design and development work" on the revisions to the J-Standard "until development and installation of the 'core' J-STD-025 features is complete." TIA Comments at 18. We believe, however, that many manufacturers already have engineers working on the design and development of CALEA solutions that include law enforcement's punch list items. Moreover, the engineers who are responsible for designing software ordinarily are assigned to new projects at the beginning of the testing phase. As a result, TIA's scenario, in which manufacturers cannot begin to deal with the punch list items until they are finished with the core J-Standard capabilities, does not provide an accurate picture of how the development process will work.

Several commenters argue that implementing modifications to the J-Standard will jeopardize other industry tasks, such as dealing with the "Y2K" problem, Local Number Portability, the E911 initiative, and so forth. We do not mean to disparage these other initiatives, all of which are important in their own right. Nevertheless, the suggestion that implementing the Commission's

order "may be the straw that breaks the regulatory camel's back" (CTIA Comments at 18) has an air of hyperbole about it. If the need to deal with issues like Y2K, LNP, and E911 has not prevented industry from continuing to develop and implement new features and services for their customers; neither should it excuse industry from taking the steps needed to meet its statutory obligations under CALEA. We do not share the industry commenters' apparent view that the interests served by CALEA must take a back seat to other industry concerns. What is at stake in this proceeding is law enforcement's ability to use legally authorized electronic surveillance to protect the public safety and security by detecting, preventing, and prosecuting criminal activities. These are interests of paramount importance, as the declarations of FBI Director Freeh and DEA Administrator Constantine underscore, and they should not be consigned to second-class status in the allocation of industry resources.

2. Several commenters argue not only that the Commission should allow a lengthy period for implementation of the new assistance capabilities, but that the current, already-extended deadline for implementation of the J-Standard -- June 30, 2000 -- should be extended yet again to coincide with the deadline for the new capabilities. See, e.g., CTIA Comments at 19; Nextel Comments at 25; Bell Atlantic Mobile Comments at 13-14. These commenters suggest that a single (and, needless to say, late) compliance deadline would be more "efficient" than separate deadlines for the core J-Standard and the capabilities that are added in this proceeding.

When the Commission issued its order in September 1998 granting an industry-wide extension of the date by which the obligations of Section 103 will become effective, the Commission stressed that the new deadline of June 30, 2000, was a "firm" one. Extension Order ¶ 46. It is hardly surprising, but nevertheless regrettable, that the industry is already inviting the Commission to

abandon that deadline in favor of a substantially later one. We urge the Commission to reject this invitation and reiterate that the existing deadline is a firm one that will not be changed.

The current industry comments indicate that while individual carriers may encounter obstacles in meeting the June 2000 deadline, there is no reason to think that the industry as a whole will be unable to meet that deadline. For example, TIA states that "[w]ireline, cellular and broadband PCS manufacturers are working closely to comply with the Commission's extension of the compliance deadline for the 'core' J-STD-025," and suggests that only "individual" petitions for extension may be necessary. TIA Comments at 19 n.42. No commenter even attempts to argue that compliance with the June 2000 deadline is beyond the reach of all carriers. As a result, the Commission should make clear that any requests to extend the current deadline will be entertained only on a carrier-specific rather than industry-wide basis.²⁹

The suggestion that it would be more "efficient" to have a single compliance deadline is inconsistent with our understanding of how manufacturers expect to provide their CALEA solutions to carriers. We understand that manufacturers generally intend to rely on a phased deployment, in which CALEA capabilities are made available over a series of several generic upgrades. Having one deadline for the "core" J-Standard capabilities and a subsequent deadline for the additional capabilities is consistent with this phased deployment model.

²⁹ GTE suggests that the Commission give the Chief of the Common Carrier Bureau authority to grant nine-month extensions of the implementation deadline, based on showings of "need" by individual carriers. GTE Comments at 16. However, CALEA provides that requests for extensions will be acted on by the Commission itself, in "consultation with the Attorney General," rather than being delegated to one of the Commission's bureaus. 47 U.S.C. § 1006(c)(2).

Moreover, the suggestion that the Commission delay the deadline for implementing the J-Standard takes no account whatsoever of the law enforcement requirements that underlie CALEA. Congress enacted CALEA in 1994. Even with the existing deadline, wireline and cellular/PCS carriers will not implement the core J-Standard until mid-2000, nearly 6 years after CALEA was enacted. The technical obstacles to electronic surveillance that led Congress to enact CALEA in 1994 are no less pressing today than they were then; to the contrary, they grow more pressing every day. To extend the compliance deadline yet again would compound law enforcement's growing inability to employ authorized electronic surveillance of modern telecommunications networks to protect public safety and security. The public has a vital interest in seeing that the Commission avoid that result.

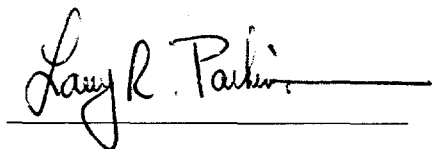
DATE: January 27, 1999

Respectfully submitted,


Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Donald Remy
Deputy Assistant Attorney General

A handwritten signature in cursive script, reading "Larry R. Parkinson", followed by a horizontal line.

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

A handwritten signature in cursive script, reading "Douglas N. Letter", followed by a horizontal line.

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)

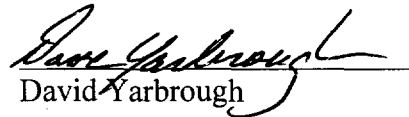
Communications Assistance for Law)
Enforcement Act)
_____)

CC Docket No. 97-213

Certificate of Service

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), Washington, D.C., hereby certify that, on January 27, 1999, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Reply Comments Regarding Further Notice of Proposed Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Washington, D.C. this 27th day of January, 1999.


David Yarbrough

**IN THE MATTER OF:
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT
CC DOCKET 97-213
SERVICE LIST**

***The Honorable William E. Kennard
Chairman
Federal Communications Commission
445 12th Street, S.W., Room 8B201
Washington, D.C. 20554**

***The Honorable Harold Furchtgott-Roth
Commissioner
Federal Communications Commission
445 12th Street, S.W., Room 8A302
Washington, D.C. 20554**

***The Honorable Susan Ness
Commissioner
Federal Communications Commission
445 12th Street, S.W., Room 8B115
Washington, D.C. 20554**

***The Honorable Michael Powell
Commissioner
Federal Communications Commission
445 12th Street, S.W., Room 8A204
Washington, D.C. 20554**

***The Honorable Gloria Tristani
Commissioner
Federal Communications Commission
445 12th Street, S.W., Room 8C302
Washington, D.C. 20554**

***Ari Fitzgerald
Legal Advisor to Chairman Kennard
Federal Communications Commission
445 12th Street, S.W., Room 8B201
Washington, D.C. 20554**

***James Casserly**
Legal Advisor to Commissioner Ness
Federal Communications Commission
445 12th Street, S.W., Room 8B115B
Washington, D.C. 20554

***Paul E. Misener**
Senior Legal Advisor to Commissioner Furchtgott-Roth
Federal Communications Commission
445 12th Street, S.W., Room 8A302B
Washington, D.C. 20554

***Peter A. Tenhula**
Legal Advisor to Commissioner Powell
Federal Communications Commission
445 12th Street, S.W., Room 8A204F
Washington, D.C. 20554

***Karen Gulick**
Legal Advisor to Commissioner Tristani
Federal Communications Commission
445 12th Street, S.W., Room 8C302F
Washington, D.C. 20554

***Christopher J. Wright**
General Counsel
Federal Communications Commission
445 12th Street, S.W., Room 8C755
Washington, D.C. 20554

***Lawrence E. Strickling**
Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street N.W., Room 500
Washington, D.C. 20554

***Gerald Vaughan**
Acting Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

*Thomas Sugrue
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

*Anna Gomez
Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street N.W., Room 235B
Washington, D.C. 20554

*Kent Nilsson
Office of Engineering and Technology
Federal Communications Commission
2000 M Street N.W.
Washington, D.C. 20554

*Charles Iseman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 424
Washington, D.C. 20554

*Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 281
Washington, D.C. 20554

*Julius Knapp
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 425
Washington, D.C. 20554

***Rodney Small**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 480
Washington, D.C. 20554

***Geraldine Matise**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 480
Washington, D.C. 20554

***Charlene Lagerwerff**
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 8633
Washington, D.C. 20554

***James Green**
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 7021
Washington, D.C. 20554

***Tejal Mehta**
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 7115
Washington, D.C. 20554

***David O. Ward**
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street, N.W., Room 210
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
Suite 300
2500 Wilson Boulevard
Arlington, VA 22201-3834

Stewart A. Baker
Tom Barba
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
Suite 200
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Mark J. Golden
Senior Vice President, Industry Affairs
Robert Hoggarth
Senior Vice President, Paging/Messaging
Personal Communications Industry Association
Suite 700
500 Montgomery Street
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry Solutions
Suite 500
1200 G Street, N.W.
Washington, D.C. 20005

Jerry Berman
Executive Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
Room 3252F3
295 North Maple Avenue
Basking Ridge, NJ 07920

William L. Roughton, Jr.
Associate General Counsel
PrimeCo Personal Communications, L.P.
Suite 320 South
601 13th Street, N.W.
Washington, D.C. 20005

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Washington, D.C. 20036

Joseph R. Assenzo
4900 Main Street, 12th Floor
Kansas City, MO 64112

James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
Suite 200
1320 18th Street, N.W.
Washington, D.C. 20036

Lisa S. Dean
Director, Center for Technology Policy
Free Congress Foundation
717 Second Street, N.E.
Washington, D.C. 20002

Anita Sheth
Director, Regulatory Policy Studies
Citizens for a Sound Economy
Suite 700
1250 H Street, N.W.
Washington, D.C. 20005

James X. Dempsey
Senior Staff Counsel
Daniel J. Weitzner
Deputy Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Lawrence E. Sarjeant
Linda Kent
Keith Townsend
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President, Regulatory Policy and Law
Cellular Telecommunications Industry Association
Suite 200
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

John Pignataro
Senior Technical Advisor
Police Department, City of New York
Fort Totten Building 610
Bayside, NY 11359

Barbara J. Kern
Counsel
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

Robert Vitanza
Suite 1300
15660 Dallas Parkway
Dallas, TX 75248

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
Suite 1700
1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610

Michael P. Goggin
BellSouth Cellular Corp.
Suite 910
1100 Peachtree Street, N.E.
Atlanta, GA 30309-4599

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Charles M. Nalborne
Suite 400
3353 Peachtree Road, N.E.
Atlanta, GA 30326

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Kathryn Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, D.C. 20036

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas Meeds LLP
Suite 500
1735 New York Avenue, N.W.
Washington, D.C. 20006

John M. Goodman
Attorney for the Bell Atlantic telephone companies
1300 I Street, N.W.
Washington, D.C., 20005

Francis D. R. Coleman
Director of Regulatory Affairs- North America
ICO Global Communications
1101 Connecticut Avenue, NW
Suite 550
Washington, D.C. 20036

Cheryl A. Tritt
James A. Casey
Morrison & Foerster LLP
2000 Pennsylvania Avenue, N.W.
Suite 5500
Washington, D.C. 20006

Joel M. Margolis
Corporate Counsel-Regulatory
Nextel Communications, Inc.
1505 Farm Credit Drive
Suite 100
McLean, Virginia 22102

Sylvia Lesse
Marci Greenstein
Kraskin, Lesse & Cosson, LLP
2120 L Street, N.W.
Suite 520
Washington, DC 20037

Robert M. Lynch
Roger K. Toppins
Hope E. Thurrott
One Bell Plaza, Room 3023
Dallas, Texas 75202

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Henry M. Rivera
Larry S. Solomon
J. Thomas Nolan
Shook, Hardy & Bacon LLP
1850 K Street, N.W.
Suite 900
Washington, D.C. 20006

Colette M. Capretz
Fisher Wayland Cooper
Leader & Zaragoza LLP
2001 Pennsylvania Ave., N.W.
Suite 400
Washington, D.C. 20006

Lon C. Levin
Vice President and Regulatory Counsel
American Mobile Satellite Corporation
10802 Park Ridge Boulevard
Reston, Virginia 20191

Carole C. Harris
Christine M. Gill
Anne L. Fruehauf
McDermott, Will & Emery
600 Thirteenth St., N.W.
Washington, D.C. 20005

Peter M. Connolly
Koteen & Naftalin, LLP
1150 Connecticut Ave., N.W.
Washington, D.C. 20036

Edward J. Wisniewski
Deputy Assistant Administrator
Office of Investigative Technology
Drug Enforcement Administration
8198 Terminal Road
Lorton, VA 22079

Dudley M. Thomas
Director
Texas Department of Public Safety
5805 N. Lamar Blvd.
Box 4087
Austin, Texas 78773-0001

Colonel Carl A. Williams
Superintendent, New Jersey State Police
Post Office Box 7068
West Trenton, NJ 08628-0068

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

* Hand Delivered